NATOのサイバー軍と日本の自衛隊

JCA-NET セミナー
小倉利丸
2023/5/26

NATOと日本の関係

- 現在、ロシア・ウクライナ戦争ではウクライナの「IT軍」の動向に関心が集まっている。IT軍は、10万から20万のメンバーを世界中から集めており、日本からの参加者もいる。パソコン1台あればサイバー攻撃の当事者になれるというハードルの低さがあり、自分がやっていることの結果を自覚しづらいことも問題だ。こうした事態と9条のような伝統的な戦争を前提にした戦争概念との乖離がいちじるいい状況になっている。
- NATOと日本の関係
  - NATOサイバー防衛演習：ロックド・シールズ
  - NATOサイバー防衛演習：Cyber Coalition22
- 防衛省の動向
- 国際法
  - NATO:タリン・マニュアル
  - 国連の動向
- まとめ

NATOと日本の関係

- **「ＮＡＴＯサイバー防衛協力センターの活動への正式参加について」防衛省**

https://www.mod.go.jp/j/press/news/2022/11/04b.html

防衛省・自衛隊として、サイバー分野における諸外国等との協力の強化について取り組んできたところ、ＮＡＴＯ承認の研究機関であるＮＡＴＯサイバー防衛協力センターとの協力について、今年１０月に同センターの活動への参加に係る手続が完了し、防衛省は正式に同センターの活動に参加することとなりました。

同センターは、サイバー行動に適用され得る国際法についての研究プロジェクトの成果として、「タリン・マニュアル」を発表しています。我が国は、サイバー分野における国際的な規範の形成に係る議論に積極的に関与する方針であり、同センターの取組は我が国の立場とも整合するものです。

防衛省・自衛隊は、２０１９年から同センターに職員を派遣しており、また、２０２１年以降、同センターが主催するサイバー防衛演習「ロックド・シールズ」に正式参加しています。これらのような取組を通じて、ＮＡＴＯ諸国を始めとする諸外国等とのサイバー分野における協力を一層強化していきたいと考えています。

同センターにはＮＡＴＯ加盟国以外にオーストラリア、韓国などが参加。２０１９年から同センターに防衛省職員１人を派遣していた。

- **NATO事務総長　連絡事務所を東京に開設へ　日本政府と協議**

ストルテンベルグ事務総長が10日、CNNテレビのインタビュー

ロシアや中国への対応を念頭に、NATOとインド太平洋地域の国々との連携を強化する必要があると強調

https://www3.nhk.or.jp/news/html/20230511/k10014063711000.html

NATOと日本の関係

「ＮＡＴＯサイバー防衛協力センターの活動への正式参加について」防衛省

「ＮＡＴＯ承認の研究機関である」は意図的に誤解を与えようとした表現だ

センターのウエッブには以下の記述がある。

「CCDCOEは、2008年5月14日に他の6か国--ドイツ、イタリア、ラトビア、リトアニア、スロバキア共和国、スペイン--とともにエストニアの主導で設立された。北大西洋評議会は、同じ年の10月にセンターに完全な認定と国際軍事組織の地位を授与することを決定した。」つまり、センターはれっきとした軍事組織の地位をNATOの最高意思決定機関である大西洋評議会自身が授与している。この事実を防衛省は「研究機関」と位置づけるという意図的と思われるミスリードによって、隠蔽した。ちょうど22年11月は安保防衛3文書の議論の渦中だったはずだ。この時期に加盟したのは、安保防衛3文書の成立を見越して、自体を先取りしたといえる。

防衛省が言及していないこととして、日本と同時にウクライナも正式加盟した点だ。ウクライナは、センターへの加盟をNATO正式加盟への第一歩と位置づけている。

https://ccdcoe.org/news/2023/the-nato-ccdcoe-welcomes-new-members-iceland-ireland-japan-and-ukraine/

【参考】サイバー攻撃対処等を含む情報通信分野におけるその他関係国との連携

NATO

○ **日NATOサイバー防衛スタッフトークス**
- サイバー空間を巡る諸課題について相互に紹介、意見交換を実施。
- 議長：〔日側〕防衛政策局戦略企画課長 〔NATO側〕NATO新規安全保障課題局サイバー防衛課長

○ **NATO主催の多国間サイバー演習への参加**
- ２０１９年、２０２２年にNATO主催の多国間サイバー演習「サイバー・コアリション(Cyber Coalition)」に正式参加

○ **NATOサイバー防衛協力センター（CCDCOE *1）との協力** （*1 Cooperative Cyber Defence Centre of Excellence)
- ２０２１年、２０２２年にCCDCOE主催の多国間サイバー演習「ロックド・シールズ(Locked Shields)」に正式参加
- CCDCOE主催のサイバー紛争に関する国際会議(CyCon *2)への参加 （*2 International Conference on Cyber Conflict)
- ２０２２年１０月、防衛省は正式に同センターの活動に参加(２０１９年３月～２０２２年３月に防衛省職員１名、２０２２年８月以降、他の防衛省職員１名を派遣中。)

欧州（２国間）

○ **防衛当局間によるサイバー協議（英国、ドイツ、フランス、エストニア）**

ASEAN

○ **日ASEANサイバーセキュリティ能力構築支援事業**

ベトナム

○ **日越ＩＴフォーラム**
- サイバーセキュリティを含む情報通信分野の取組及び技術動向に関する意見交換を実施。これまで８回開催
- 議長：〔日側〕整備計画局情報通信課長 〔越側〕国防省サイバー空間作戦司令部司令

○ **日越防衛当局間「サイバーセキュリティ分野での協力に関する覚書」（2021年１１月署名）**

https://www.mod.go.jp/j/policy/hyouka/rev_gaibu/pdf/2023_01_siryo_055.pdf

【参考】サイバー政策に係る日米間協力の枠組み等

日米サイバー防衛協力について

- 近年、サイバー攻撃の態様は、より一層複雑化・巧妙化・高度化。また、国境を越えるサイバー空間の脅威に対しては、国際的に連携して対処していく必要。
- サイバー攻撃は、自衛隊や米軍の任務遂行の場面において大きな阻害要因等となり得ることから、今後日米防衛協力を一層推進していく上で、サイバー空間の安定的かつ効果的な利用の確保は重要。

日米サイバー協力の主要枠組み

日米サイバー対話

（政府間の包括的協議。7回開催）

日米ITフォーラム

（防衛当局間の情報通信分野に関する協議。１５回開催）

日米サイバー防衛政策ワーキンググループ(CDPWG)

（防衛当局間の政策協議。８回開催）

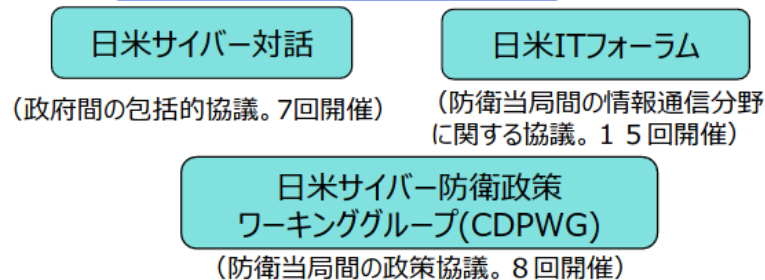
脅威情報の共有

重大事案への共同対処

両政府全体の取組＋自衛隊・米軍による取組

日米サイバー協力の深化

重要インフラの防護

共同演習

日米サイバー防衛協力の主要成果

日米防衛協力のための指針（２０１５年4月）

➢ サイバー空間に関する協力の項を新たに設け、情報共有等、今後の日米のサイバー協力に関する方向性を記述

日米ｻｲﾊﾞｰ防衛政策ﾜｰｷﾝｸﾞｸﾞﾙｰﾌﾟ(CDPWG)共同声明（２０１５年5月）

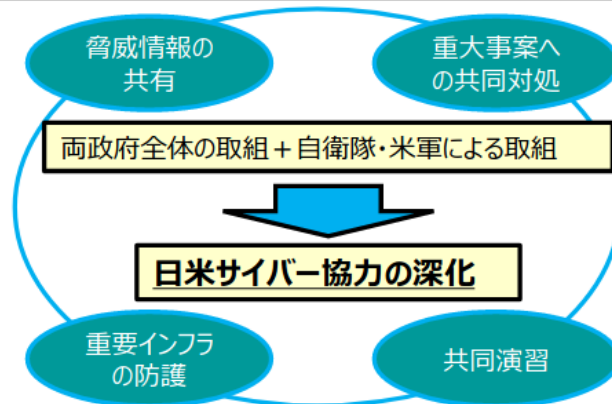
➢ サイバーに係る脅威認識を共有した上で、重大なサイバー事案への対処、役割・任務、情報共有、重要インフラ防護等、防衛省・国防省間における具体的な協力分野を記述。

日米「２＋２」共同発表（２０１９年４月）

➢ サイバー分野における協力を強化していくことで一致し、国際法がサイバー空間に適用されるとともに、一定の場合には、サイバー攻撃が日米安全保障条約第５条にいう武力攻撃に当たり得ることを確認。

日米「２＋２」共同発表（２０２３年１月）

➢ 閣僚は、同盟にとっての、サイバーセキュリティ及び情報保全の基盤的な重要性を強調した。閣僚は、２０２２年３月の自衛隊サイバー防衛隊の新編を歓迎し、更に高度化・常続化するサイバー脅威に対抗するため、協力を強化することで一致した。米国は、より広範な日米協力の基盤を提供することとなる、政府全体のサイバーセキュリティ政策を調整する新たな組織の設置及びリスク管理の枠組みの導入など、国家のサイバーセキュリティ態勢を強化する日本のイニシアティブを歓迎した。閣僚は、日本の防衛産業サイバーセキュリティ基準の策定に係る取組を含む、産業サイバーセキュリティ強化の進展を歓迎した。そして、閣僚は、情報保全に関する日米協議の下でのこれまでの重要な進展を強調した。

4

https://www.mod.go.jp/j/policy/hyouka/rev_gaibu/pdf/2023_01_siryo_055.pdf

１１．日・ＮＡＴＯ国別パートナーシップ協力計画

- 日・NATO国別パートナーシップ協力計画（IPCP：Individual Partnership and Cooperation Programme）は、日・NATO協力の主要な指針、協力の原則及び協力分野等を整理した文書。
- 2014年5月、安倍総理とラスムセン事務総長（いずれも当時）がIPCPに署名。政治対話や防衛交流の促進に加え、日・NATO間で以下の優先分野に焦点を当てた実務的な協力を促進していくことを確認。
- 2022年6月、岸田総理はストルテンベルグ事務総長と会談を行い、IPCPを新時代にふさわしいものにアップグレードし、新たな協力文書の早期合意に向けて作業を加速することを確認。

日・NATO協力の優先分野

① サイバー防衛
② 海洋安全保障
③ 人道支援・災害救援
④ 小型武器を始めとする通常兵器、大量破壊兵器及びその運搬手段に関する軍備管理、不拡散及び軍縮
⑤ 防衛科学技術
⑥ 女性・平和・安全保障
⑦ 人間の安全保障
⑧ パブリック・ディプロマシー活動
⑨ 日本及びNATOの共通関心分野における防衛及び安全保障に関するその他の協力

実務的な協力の例

分野	内容
サイバー防衛	➢ 2019年3月より、エストニアにあるNATOサイバー防衛協力センター（CCDCOE）へ防衛省職員を派遣。 ➢ 2019年12月、NATOサイバー防衛演習（サイバー・コアリション）に初めて正式に参加。 ➢ 2021年4月、CCDCOEが主催するサイバー防衛演習（ロックド・シールズ）に初めて正式に参加。2022年4月にも、英国と合同チームを編成して参加。
海洋安保	➢ 2014年9月及び11月にソマリア沖アデン湾で、自衛隊とNATOオーシャンシールド参加部隊が海賊対処共同訓練を実施。直近では、2022年6月に自衛隊とNATO第2常設海上部隊と共同訓練を実施。 ➢ 2019年6月より、NATO海上司令部（MARCOM）へ海上自衛隊より連絡官（在英国防衛駐在官）を派遣。
人員交流	➢ 2019年11月、NATO本部諮問・指揮統制幕僚部に対して3代目となる女性自衛官を派遣（2代目までは女性・平和・安全保障（WPS）オフィスへ派遣）。2021年11月、4代目となる女性自衛官をNATO本部国際機関/NGO協力オフィスに対して派遣。
拠出	➢ ウクライナ不発弾処理プロジェクトやジョージア・サイバー防衛研究所プロジェクト等、平和のためのパートナーシップ信託基金や防衛能力構築支援信託基金への拠出を通じた支援。 ➢ 殺傷性のない装備品支援のため、「ウクライナのための包括的支援パッケージ（CAP）」信託基金に拠出。
オペレーション	➢ トルコ南東部を震源とする地震被害に対し、日本の自衛隊機がNATO主導の災害救援物資の空輸オペレーションに史上初めて参加。

ロックド・シールズ2022（於：タリン）
出典：NATO HP

日NATO共同訓練（2022年6月）
出典：自衛隊プレスリリース

11

「北大西洋条約機構（ＮＡＴＯ）について」
2023年4月
外務省欧州局政策課
https://www.mofa.go.jp/mofaj/files/100156880.pdf

NATOサイバー防衛演習：ロックド・シールズ

日本は、ここ3年間NATOの「ロックド・シールズ」と呼ばれるサイバー戦争の演習に正式に参加している

防衛省
ＮＡＴＯサイバー防衛協力センターによるサイバー防衛演習『ロックド・シールズ２０２３』への参加について

NATOのサイトの告知の日本語訳

参加組織の構成

- 自衛隊の各部隊
- 政府省庁：内閣官房内閣サイバーセキュリティセンター（ＮＩＳＣ）、総務省、警察庁、情報処理推進機構（ＩＰＡ）、ＪＰＣＥＲＴコーディネーションセンター（ＪＰＣＥＲＴ／ＣＣ）
- 「重要インフラ事業者等」として民間からの参加

NATOサイバー防衛演習：ロックド・シールズ

１　目的　ＮＡＴＯサイバー防衛協力センター（ＣＣＤＣＯＥ）が主催するサイバー防衛演習「ロックド・シールズ２０２３」に参加し、サイバー攻撃への対処能力向上及びサイバーセキュリティ動向の把握を図る。 ※ＣＣＤＣＯＥ = Cooperative Cyber Defence Centre of Excellence

２　参加時期

2023年４月１８日（火）から同月２１日（金）まで

３　実施場所

防衛省等　※演習統裁部はタリン（エストニア）に置かれるが、演習参加者は自国からオンライン形式で参加

４　演習参加予定国（日本以外）　ＮＡＴＯ加盟国を含む約４０か国

５　参加部隊等

（１）防衛省　内部部局、統合幕僚監部、陸上自衛隊システム通信団、海上自衛隊システム通信隊群、航空自衛隊作戦システム運用隊、航空自衛隊航空システム通信隊、自衛隊サイバー防衛隊

（２）他府省等　内閣官房内閣サイバーセキュリティセンター（ＮＩＳＣ）、総務省、警察庁、情報処理推進機構（ＩＰＡ）、ＪＰＣＥＲＴコーディネーションセンター（ＪＰＣＥＲＴ／ＣＣ）、重要インフラ事業者等

（３）豪州（※）　豪国防省　※　本年は豪州と合同チームを編成して参加。

６　本演習への参加実績

２０２１年４月：「ロックド・シールズ２０２１」　２０２２年４月：「ロックド・シールズ２０２２」

https://www.mod.go.jp/j/press/news/2023/04/18d.html

NATOサイバー防衛演習：ロックド・シールズ

BERYLIA
CRIMSONIA
LOCKED SHIELDS 2023
2:17 / 2:30

。

NATOサイバー防衛演習：ロックド・シールズ

防衛省・自衛隊
@ModJapan_jp

４月１９日に #井野防衛副大臣 が、２０日に #小野田防衛大臣政務官 が、それぞれ「ロックド・シールズ2023」を視察しました。防衛省・自衛隊は、本演習で合同チームを組む豪州🇦🇺を含む同志国等とともにサイバー防衛の強化を図ります🤝
#CCDCOE #LockedShields2023

午後7:23 · 2023年4月25日 · 8.9万 件の表示

資料収集で一部下記を参照
#LockedShields 国際サイバー防衛演習「ロックド・シールズ」2023をまとめてみたJAPAN(=・ω・)R5
https://togetter.com/li/2132211

NATOサイバー防衛演習：ロックド・シールズ

NTT広報

国際サイバー防衛演習「Locked Shields 2023」にNTTグループが参加

「NTTグループは、4月18日から21日まで開催される、NATOサイバー防衛協力センター（CCDCOE: Cooperative Cyber Defence Centre of Excellence）主催の国際サイバー防衛演習「Locked Shields 2023」に参加します。

NTTドコモ、NTTコミュニケーションズ、NTTデータ、ならびにNTTセキュリティ・ジャパンにとって、今回は昨年に引き続き、2度目の参加になります。本演習は、約40か国が参加し、架空の国に対するサイバー攻撃を想定して行われるものです。

日本チームは、同志国や団体との連携を深め、サイバーインシデント対応能力を共同で強化するため、今回は、オーストラリアとチームを組み、日本の政府機関や民間企業、オーストラリア国防省とともに参加します。」

NATOサイバー防衛演習：ロックド・シールズ

2023年は4月18日（火曜日）～21日（金曜日）の日程で開催され、NATO加盟国を含む約40か国が参加しました。日本からは防衛省・自衛隊のほか、内閣サイバーセキュリティセンター（NISC）、総務省及び警察庁、重要インフラ関連などの企業が参加し、IPA 産業サイバーセキュリティセンター（ICSCoE）が運営する「中核人材育成プログラム」（以下、同プログラム）の修了者17名を含む総勢約120名が日豪合同チームとして演習を行いました。

演習では5、500の仮想システムに対し8、000以上の大規模なサイバー攻撃が行われ、重要インフラ等のシステムを攻撃から防護する技術的な対処やインシデントの報告のほか、法務、広報、情報活動に関する課題への対処を含む総合的な対応スキルを24のブルーチームで競いました。

日本チームは官民や同志国との連携によりインシデント対応を演習し、日本国内の重要インフラ企業でサイバーセキュリティ戦略の実務を担う同プログラムの修了者たちは、約一年間のプログラムで習得した高度なセキュリティ技術に関する知見や、自社での実務経験などを活かしながらチームの成果に貢献しました。

同プログラムの修了者の参加は今回で3回目となり、本演習への継続的な参加によって得られる、組織的なインシデント対応に関する知見のアップデートやスキルの向上が、日本国内の重要インフラにおけるサイバーリスクの低減につながることが期待されます。

IPA 独立行政法人 情報処理推進機構

IPAについて

情報セキ

「ロックド・シールズ2023」に中核人材育成プログラムの修了者が参加しました

参加した中核人材育成プログラムの修了者

https://www.ipa.go.jp/jinzai/ics/global/locked-shields2023.html

NATOサイバー防衛演習：ロックド・シールズ

中部電力パワーグリッド　停電情報　雷情報　でんき予報　ニュース　よくあるご質問・お問い合わせ

ご案内　安定供給　サービス・ソリューション　効率化・低コスト化

ホーム ＞ ニュース ＞ お知らせ ＞ NATOサイバー防衛協力センター主催のサイバー防衛演習「ロックド・シールズ2023」への参加

お知らせ

お知らせ

NATOサイバー防衛協力センター主催のサイバー防衛演習「ロックド・シールズ2023」への参加

2023年05月19日
中部電力パワーグリッド株式会社

印刷　記事をシェアする

当社は、サイバー攻撃への対処能力向上や最新のセキュリティ動向の知見を深めるため、4月18日から21日に開催されたNATO（北大西洋条約機構：North Atlantic Treaty Organization）サイバー防衛協力センターが主催するサイバー防衛演習「ロックド・シールズ2023」に参加しました。

「ロックド・シールズ」は、世界最大規模のサイバー防衛演習であり、今回はNATO加盟国を含む約40か国が参加しました。日本からも防衛省・自衛隊を始めとする関係省庁や民間事業者などが2021年より参加しており、当社も2021年から今回で3回目の参加となります。

当社は、本演習にて得られたサイバー攻撃対応、技術などの知見を活用し、サイバーセキュリティ強化に努めることで、産業界のサイバーセキュリティ向上に貢献してまいります。

＜参考＞
NATOサイバー防衛協力センターによるサイバー防衛演習「ロックド・シールズ2023」への参加について、防衛省ホームページ

COLUMN　サービスTOPICS

NEWS

2023.05.25

NATOサイバー防衛協力センター主催のサイバー防衛演習 「Locked Shields 2023」に当社社員が参加しました

#サイバー攻撃　#セキュリティ　#セキュリティ対策　#制御システム

Locked Shields 2023参加報告

2023年4月18日から21日にかけて開催された、NATOサイバー防衛協力センター（CCDCOE：Cooperative Cyber Defence Centre of Excellence）主催の国際サイバー防衛演習「Locked Shields（ロックド・シールズ） 2023」に、当社の叶野 孝文、小柳 くるみの2名が参加しました。当社としては、昨年に引き続き2度目の参加となります。

https://service.toinx.co.jp/tsq/news_003#heading-1

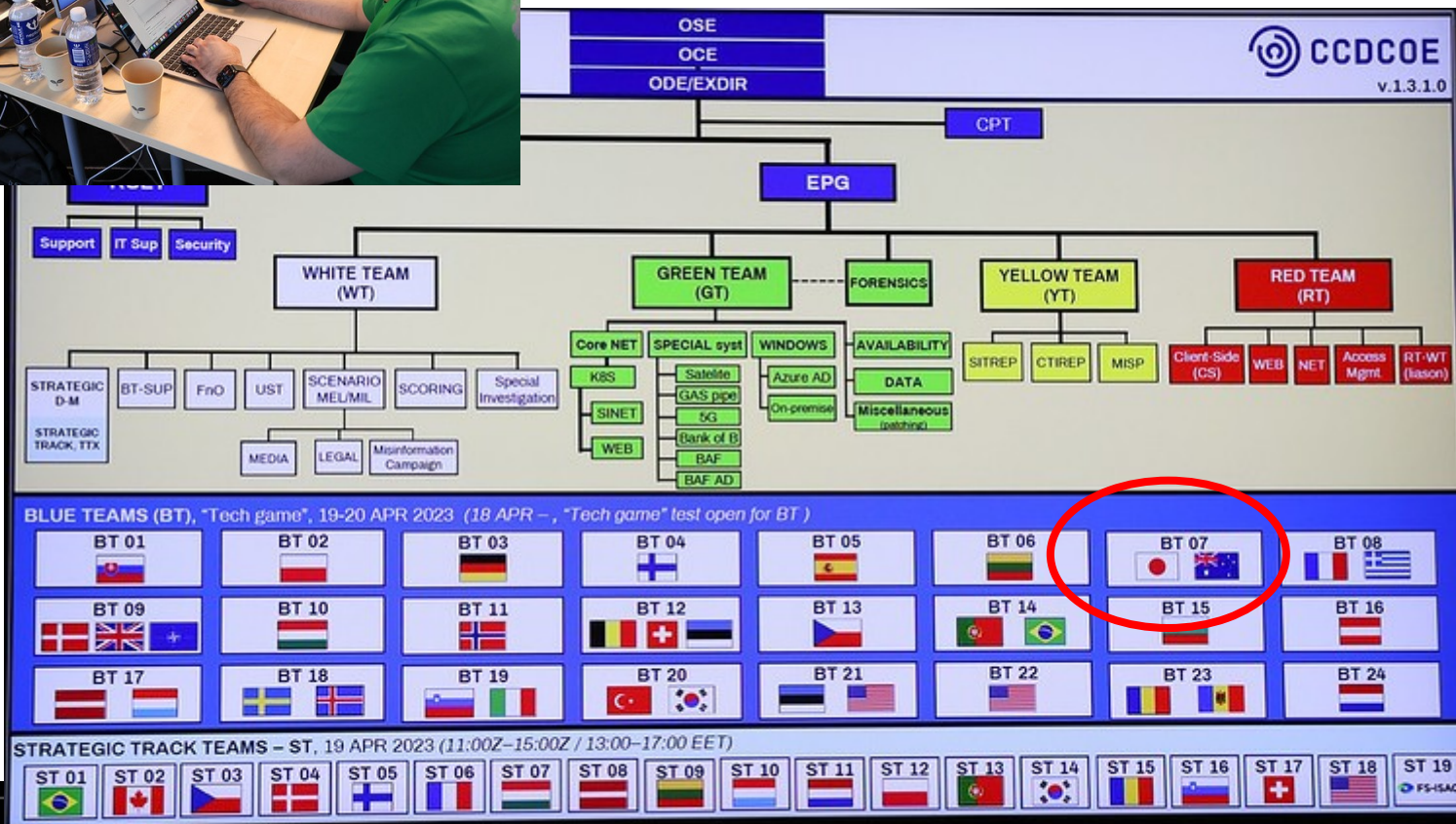
東北電力グループのIT企業

NATOサイバー防衛演習：ロックド・シールズ

政府関連の機関のJPCERTは毎年参加レポートを公開している。(23年はまだ公表されていない)

https://blogs.jpcert.or.jp/ja/2022/05/locked-shields-2022.html

日本はオーストラリアとチームを組む。
日豪のロックシールドでのチーム結成については、昨年12の第１０回日豪外務・防衛閣僚協議（「２＋２」）共同声明でも言及された。

出典 。

NATOサイバー防衛演習：ロックド・シールズ

NATO の大規模サイバー演習：Cyber Coalition 22 の開催とウクライナへの意識

。

オリジナル：。

2022/12/02 InfoSecurity -- 今週に NATO は、加盟国間のサイバー耐性強化を目的とする、Cyber Coalition 22 演習を開始した。この軍事同盟には、加盟国26カ国に加え、フィンランド／スウェーデン／ジョージア／アイルランド／スイス／日本／EU から 1000人の防衛担当者が集まり、産業界や学術界からも参加者が集まった。５日間にわたる演習は、電力網や NATO の資産に対するサイバー攻撃といった、現実的な課題を参加者に与え、ネットワークを守り、サイバースペースでの協力能力を強化することを目的にしているとのことだ。

NATOサイバー防衛演習：Cyber Coalition 22

NATO の大規模サイバー演習：Cyber Coalition

サイバー連合Cyber Coalitionは、NATOの主要な年次集団サイバー防衛演習であり、世界最大の演習の一つだ。the Military Committeeのガバナンスの下、Allied Command Transformationによって計画・実施

- 実施拠点：エストニア・サイバーセキュリティ演習・訓練センター「CR14」を通じて実施
- 目的：軍事および民間団体のためのサイバー空間作戦を実施する同盟の能力を強化
- 規模：世界中に分散する31のNATO同盟国、いくつかのパートナー、および欧州連合から約1、000人が参加。NATO通信情報局、Cooperative Cyber Defence Centre of Excellence、Joint Warfare Centre、Allied Joint Force Command Brunssum、NATO本部、産業界、学界の複数の団体など

https://act.nato.int/articles/exercise-cyber-coalition-2022-concludes-estonia

NATOサイバー防衛演習：Cyber Coalition 22

NATO の大規模サイバー演習：Cyber Coalition22

- NATO同盟国26カ国、
- 招待国フィンランド、スウェーデン、さらにグルジア、アイルランド、日本、スイス、欧州連合から1000人以上のサイバー防衛関係者、および産業界や学界からの参加
- 実施時期：2022年11月28日から12月2日
- 場所：エストニアのタリンで行われたほか、遠隔地でも実施
- 架空の軍事基地にコンピューターベースのシステムと電力網を設置し、サイバー攻撃を受けてもそれらを稼働させ続けること
- ウクライナのインフラ（電力網を含む）に対するサイバー攻撃から得たシナリオと教訓を取り入れた
- サイバー脅威に対抗するために人工知能技術の使用を応用

。

https://www.politico.com/news/2022/12/03/nato-future-cyber-war-00072060

CYBER COALITION
NATO
OTAN
EXERCISE

NATOサイバー防衛演習：Cyber Coalition 22

NATO の大規模サイバー演習：Cyber Coalition22

米国エネルギー省（DOE）のArgonne National Laboratoryが開発した新しいAutonomous Intelligence Cyberdefense Agent（AICA）

- コンピュータや通信機器の軍事ネットワーク上で能動的かつ自律的にサイバー防衛活動を行うインテリジェント・ソフトウェア・エージェント
- 技術的に洗練された敵との紛争では、NATO軍の戦術ネットワークは激しい争いのある戦場で活動することになる。彼らと戦うために、NATOは人工的なサイバーハンター、つまり積極的なサイバー防衛に特化した知能、自律性、機動性のあるエージェントを必要としている。
- 現在のような人間のサイバー防御要員への依存は、将来の戦場では通用しなくなるだろう。 今日のような人間によるサイバー防御への依存は、将来の戦場では通用しなくなる。
- その代わりに、人間の介入が不可能な、通信が途絶える可能性のある環境で敵のマルウェアを倒すために、AICAのような人工知能を持ったエージェントが必要になる。
- 思考し、適応するマルウェアと戦うために、敵対的な推論が可能でなければならない。

自律型インテリジェントサイバー防衛エージェント（AICA）リファレンスアーキテクチャ。リリース2。0

NATOサイバー防衛演習：Cyber Coalition 22

NATO の大規模サイバー演習：Cyber Coalition 22 の開催とウクライナへの意識

Cyber Coalition 22 は、「実験とコラボレーション、そして、経験とベストプラクティスの共有のための、ユニークなプラットフォームを提供する。それぞれの参加者／組織／国々／NATO が協力することで、サイバー耐性を強化されていく」と述べている。

この演習は、毎年実施されているが、ウクライナの状況を考えると、今年の取り組みには特別な緊急性がある。

2022年4月時点という、この紛争の早い段階において Microsoft が指摘していたのは、ロシアによる侵攻直前からウクライナの標的に対して、237件ものキャンペーンが展開されていたことだ。

この中には、主に政府や重要インフラといった資産に対する、40件近い攻撃も含まれていた。キエフのテレビ塔へのミサイル攻撃が行われた 3月1日には、ウクライナの主要放送局へのサイバー攻撃も発生したように、現実の軍事作戦と同じタイミングでサイバー攻撃が生じることが多かったようだ。

しかし、別の報告によると、これまでの数カ月間にロシアが仕掛けた、前例のない激しいサイバー攻撃にもかかわらず、ウクライナ人は驚くほどよく防御していた。おそらく、2015年12月～2016年に発生した、重要インフラへの攻撃から教訓を学んでいるのだろう。

そこにも、重要な教訓がある。つまり、物理的な戦争と並行して行われるサイバー戦争が、常に有効とは限らないということだ。高度な攻撃の準備には何カ月もの準備が必要で悪が、最終的には、単に爆弾を投下するよりも影響が少ないのかもしれないと、Economist の報告書は示唆している。

NATO のサイバー連合は、エストニアの首都タリンで開催されており、参加者は他の場所からもリモートで参加している

NATOサイバー防衛演習：Cyber Coalition 22

サイバー専門家がシステム、電力網、その他の重要資産を安全かつ防御するためのAIの能力に関する国際実験も実施された

Michael Hill「NATO、サイバー攻撃から重要インフラを保護するAIの能力をテスト」2023/1/5

任務：NATO同盟国のサイバー防衛担当者6チームが、架空の軍事基地にコンピューターベースのシステムと電力網を設置し、サイバー攻撃を受けてもそれらを稼働させ続けること

米国エネルギー省（DOE）のArgonne国立研究所が開発した新しいAutonomous Intelligence Cyberdefense Agent（AICA）を利用できるチームと利用できないチームで、その差を検証

目的：重要なシステムやサービスに対するサイバー攻撃に対応するためのデータ収集やチームの支援におけるAIの効率性を検証・測定するとともに、サイバーリスクを低減するために人間と機械の連携を向上させるツールの必要性を強調すること

結果：防御に成功。攻撃パターン、ネットワークトラフィック、ターゲットシステム間の関係なども把握。

NATOサイバー防衛演習：Cyber Coalition 22

「人間だけでは、それらの複雑さや攻撃ポイントを理解することは不可能です。AIは、リスク監視の有効性と効率性を高め、最終的にはリスクの軽減とシステムの回復力を高めることを可能にします。」

Alexander Kott「自律型インテリジェントサイバー防衛エージェントのリファレンスアーキテクチャ、リリース2。0紹介」

。

「技術的に洗練された敵との紛争では、NATOの軍事ネットワークは激しく争う戦場で活動することになる。敵のマルウェアが味方のネットワークやシステムに侵入して攻撃する可能性が高い。現在のような人間によるサイバー防御への依存は、将来の戦場では通用しなくなる。その代わりに、人間の介入が不可能な、通信が途絶える可能性のある環境下で敵のマルウェアを倒すために、AICAのような人工知能エージェントが必要になる。」

人間による制御が遮断されても自律的に状況を把握して侵入者を攻撃できるような機能を備える必要がある

もういちど憲法9条を読んでおく

国権の発動たる戦争と、武力による威嚇又は武力の行使は、国際紛争を解決する手段としては、永久にこれを放棄する。

②　前項の目的を達するため、陸海空軍その他の戦力は、これを保持しない。国の交戦権は、これを認めない。

憲法9条とサイバー戦争の関係は？

「サイバー戦争」では以下の概念はどのように当て嵌まるのだろうか？

- 国権の発動としての戦争
- 武力による威嚇
- 武力の行使
- 陸海空軍その他の戦力
- 国の交戦権

「戦争」「武力」「戦力」「交戦権」などの概念がどのように適応しうるのか。

防衛省のAIについての認識と取組み

**** 防衛白書2021**

https://www.mod.go.jp/j/publication/wp/wp2021/html/n130101000.html

「いわゆる人工知能（AI）技術は、近年、急速な進展がみられる技術分野の一つであり、軍事分野においては、指揮・意思決定の補助、情報処理能力の向上に加えて、自律型無人機への搭載やサイバー領域での活用など、影響の大きさが指摘されている。

**** 新技術短期実証事業(2020)**

。

「新技術短期実証事業では、部隊等が抱える課題の速やかな解決のため、民間の技術者と運用者が一体となり、民生において実用化レベルにある先端技術の有効性を実証し、３年程度の短期間で実用化を推進します。また、本事業の成果の民間市場での活用等により、防衛向け製品価格や維持費の抑制も追求します。」

**** 「防衛省におけるAIに関する取組」令 和 ４ 年 ４ 月**

https://www8.cao.go.jp/cstp/ai/senryaku/9kai/siryo7.pdf

「防衛省としてもAI技術がゲームチェンジャーになり得るものと考えており、重点的な投資を進め、防衛用途での実装を早期に実現することが必要」

防衛省におけるAIに関する取組②

別紙に追記した防衛省の取組

具体目標	取組	取組の詳細
AIによる利活用の基礎となるデジタル・ツインの構築	装備品等の研究開発におけるDXの推進	装備品等の研究開発において、設計、数値解析、実験等の各段階においてデジタルツイン、デジタルスレッド等の導入及びその運営に必要な体制強化を図る。
	ヒューマン・デジタル・ツインを教育訓練・診断に活用するための研究開発の推進	行動・神経系のデータと神経科学的知見に基づいてヒトのデジタル・ツインを構築し、教育訓練や診断治療への応用のための研究開発を推進する。
政府機関におけるAIの導入促進に向けた推進体制の強化と、それによる行政機能の強化・改善	AIアドバイザー（役務）によるAI活用検討の支援を行い、自衛隊の活動へ寄与	AI活用促進のため、役務支援によりAIアドバイザーを契約し、各機関のAI活用方針、運用・検証体制、事業計画等に助言を行うとともに、AI活用に係るガバナンス、人材、データなどに関する方針検討を行う。
	自衛隊の活動へのAI活用推進のためAI基礎講習を実施	AI活用促進のため、各機関の職員に対し、ITリテラシー、AI、データサイエンスに関する基礎講習や、AIの画像処理等の実務講習を実施する。
我が国ならではの課題に対処するAIと我が国の強みの融合の追求	我が国の防衛に資するAI技術の適用に関する研究の推進	自衛隊、装備品等の能力強化を図るため、指揮統制、探知・識別、自律化、後方支援等の分野へのAI技術の適用に関する研究を行う。

防衛省のAIについての認識と取組み

実際には世論操作に利用することが検討されている

**** (共同)防衛省、世論工作の研究に着手 AI活用、SNSで誘導**

「<u>防衛省が人工知能（AI）技術を使い、交流サイト（SNS）で国内世論を誘導する工作の研究に着手</u>したことが9日、複数の政府関係者への取材で分かった。インターネットで影響力がある<u>「インフルエンサー」が、無意識のうちに同省に有利な情報を発信するように仕向け、防衛政策への支持を広げたり、有事で特定国への敵対心を醸成、国民の反戦・厭戦の機運を払拭</u>したりするネット空間でのトレンドづくりを目標としている。

中国やロシアなどは「情報戦」に活発に取り組む。防衛省は、日本もこの分野の能力獲得が必要だと判断した。改定される安全保障関連3文書にも、情報戦への対処力向上を盛り込む。」。

**** ＜社説＞防衛省が世論工作研究 世論操作は容認できない**

https://ryukyushimpo.jp/editorial/entry-1632283.html

**** (TBS)防衛省、フェイクニュース対策強化へ AIによる自動情報収集機能の整備も “世論誘導研究”一部報道を否定**

https://newsdig.tbs.co.jp/articles/-/227448

防衛省のAIについての認識と取組み

**** **（読売）防衛装備庁に新研究機関、先端の民生技術を活用へ…ＡＩや無人機など重点支援**

2022/10/19 05:00

https://www.yomiuri.co.jp/politics/20221019-OYT1T50002/

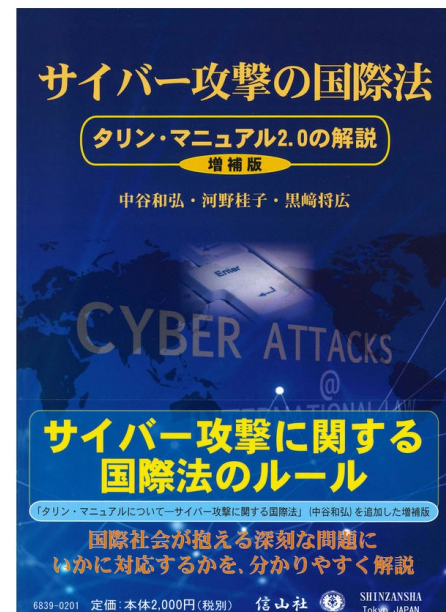
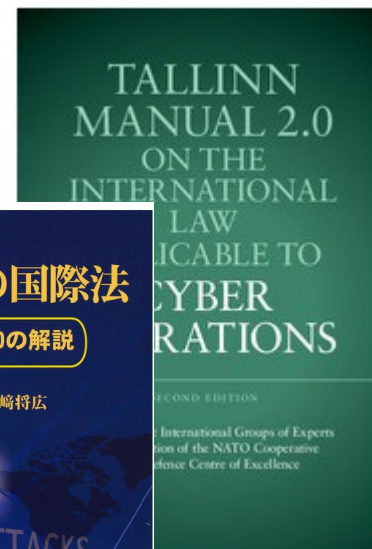
「政府は、先端の民生技術を防衛分野で活用するため、２０２４年度にも防衛装備庁に研究機関を新設する方針を固めた。ＡＩ（人工知能）や無人機など、今後の戦い方を左右する技術研究を発掘し、財政支援する。軍事と民生双方で活用できる先端技術の「デュアルユース（両用）」の研究を装備品開発につなげる狙いだ。」

「新研究機関は、大手から新興まで広範な企業や研究機関、大学などを対象に中長期的な研究費の支援を行う方向だ。公募のほか、研究機関側から支援を打診することも想定する。将来的には、年１兆円規模の支援を目指す。」

国際法関連：タリンマニュアル

以下、この項目は中谷和弘「タリン・マニュアルについて―サイバー攻撃に関する国際法―」情報処理 Vol。61 No。7 July 2020のほぼ要約である。

北大西洋条約機構（NATO）のサイバー防 衛 協 力 セ ン タ ー（Cooperative Cyber DefenceCentre of Excellence、 CCDCOE）に法律専門家が個人的資格で集まって、サイバー攻撃に関する国際法のルールをコメンタリとともに記述したもの

- サイバー攻撃の定義について「サイバー攻撃とは、攻撃としてであるか防御としてであるかを問わず、人に対する傷害若しくは死、又は物に対する損害若しくは破壊を引き起こすことが合理的に予期されるサイバー行動である」
- 「国家は、他国の主権を侵害するサイバー行動を行ってはならない」と規定する。領域外からのサイバー行動については、サイバー・インフラの物理的損害が発生した場合のみならず機能の喪失が生じた場合も主権侵害となる。政府機能の行使に必要なデータの改変・削除も主権侵害となる。

中谷和弘、河野桂子、黒﨑将広『サイバー攻撃の国際法 ― タリン･マニュアル2。0の解説【増補版】』信山社

国際法関連:タリンマニュアル

武力攻撃と自衛について

- 一定以上の「規模および効果」を有するサイバー攻撃は国際法上の「武力攻撃」に該当する。その場合には、武力攻撃を受けた国は個別的自衛権の発動が、その友好・同盟国は集団的自衛権の発動が可能となる。
- 「武力攻撃の水準に至るサイバー行動の目標となる国家は、固有の自衛権を行使することができる。サイバー行動が武力攻撃に該当するか否かは、その規模および効果による」
- 多数の人間を殺傷したり、財産に重大な損害・破壊をもたらすサイバー行動は、武力攻撃に必要な規模および効果を有する。
- 自衛権の発動としての措置は、サイバー手段によるものと非サイバー手段によるものの双方が想定される。
- 個別的自衛権の行使には、「必要性と均衡性」(規則 72) および「急迫性と即時性」(規則 73)の要件を満たす必要があり、
- 集団的自衛権の行使にはさらに「被害国の要請」(規則 74)の要件も満たす必要がある。

国際法関連：タリンマニュアル

国際法上違法な（ただし武力攻撃には至らない程度の）サイバー攻撃に対しては、被害国は対抗措置（countermeasures） をとり得る。

- 「国家は、他国が自国に対して負う国際インフラからサイバー攻撃がなされたからという事
- 法上の義務違反への反応として、対抗措置（性質上サイバーであるか否かを問わない）をとる権限を有する」
- 対抗措置には、サイバー手段によるものも想定され得るが、現実には 対抗措置の中心を成すのは経済的措置である。
- 対抗措置が容認される（＝違法性が阻却される）ためには、均衡性（規則 23 ）をはじめとする要件を満たす必要がある。
- 規則 24は、「被害国のみが対抗措置（性質上サイバーであるか否かを問わない）をとることができる」と規定する。
- 対抗措置をとることができるのは国家のみであり、たとえばサイバー攻撃を受けた企業自らが対抗措置をとることはできない。

国際法関連：タリンマニュアル

国家機関によるサイバー攻撃について。

「国家機関又は国内法によって統治権能の一部を行使する権限を付与された個人若しくは団体によってなされたサイバー行動は、当該国に帰属する」

法令や契約によって他国にサイバー攻撃を行う法的権限を付与された企業の行動も国家に責任が帰属する。

企業が権限を逸脱してハック・バックをした場合にも、その行為は国家に帰属する。

私人等の非国家主体によるサイバー攻撃

「非国家主体によってなされたサイバー行動は、次の場合に国家に帰属する。

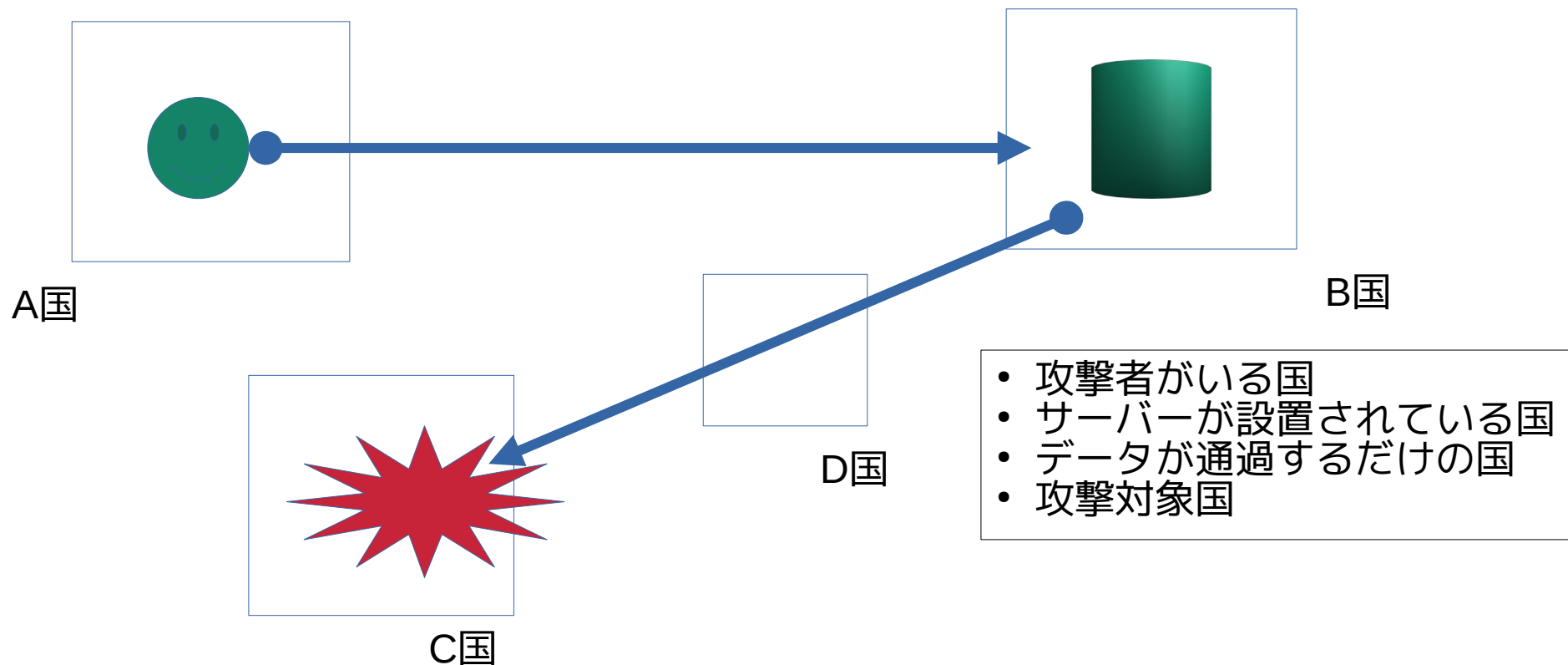
（a）その指示に従い又はその指揮若しくは命令下でなされた場合

（b）国家が当該活動を自己の活動として認め、かつ採用した場合」

非国家主体には、個人のハッカー、ハッカー集団、サイバー犯罪組織、IT 関連企業、サイバー・テロリスト、反政府勢力等が含まれる。

国際法関連:タリンマニュアル

- A 国に所在するハッカー集団が C 国にあるサイバー施設を使って B 国に対するサイバー攻撃を実施したが、C 国がそれを知りながらも攻撃を終了させるための実行可能な措置をとらなかった場合には、C 国は相当の注意原則の違反になる
- データが通過するだけの国家が相当の注意義務を負うかについては、サイバー行動を了知し、かつそれを終了させるため実行可能な措置をとれる場合には、相当の注意義務を負うが、通過国は一般には悪意あるトラフィックを了知し得ないので、相当の注意義務を負う場合は現実には例外的になる

国際法関連：タリンマニュアル

国際法関連:タリンマニュアル

- サイバー諜報(cyber espionage)

それ自体は国際法によって規律されないサイバー行動

諜報(スパイ行為)一般は、国際法上、禁止はされていないが、各国の国内法で刑事罰を科すことは可能という独自の法的性質を有している。サイバー諜報についても基本的に同様

- サイバー通信の停止について。

(a) 国家は、部分的又は完全に、自国領域内における国際サイバー通信業務を停止することができる。当該停止の即時の通知が他国に対してなされなければならない。

(b) 国家は、国内法令、公の秩序若しくは善良の風俗に反すると認められ、又は国家の安全にとって危険である私用のサイバー通信の伝達を停止することができる

個人は、サイバー関連活動に関し、他で享受するのと同じ国際人権を有する

2011 年のアラブの春のように反体制運動が SNS で広まった際に国家がサイバー通信を停止することは、国家の権利かどうか

国際法関連：タリンマニュアル

- 軍事目標主義について

「民用物はサイバー攻撃の対象とされてはならない。コンピュータ、コンピュータ・ネットワークおよびサイバー・インフラは、それらが軍事目標である場合にはサイバー攻撃の対象となる」

「民用物は、軍事目標ではないすべての物をいう。軍事目標は、その性質、位置、用途又は使用が軍事活動に効果的に資するものであってその奪取又は無効化が、その時点における状況において明確な軍事的利益をもたらすものをいう。軍事目標はコンピュータ、コンピュータ・ネットワークおよびサイバー・インフラを含み得る」

軍事目標武力紛争法の基本原則の1つである軍事目標主義は、 1949 年ジュネーヴ条約第 1 追加議定書 52 条でも規定

何でも軍事目標になりうる？

国際法関連：タリンマニュアル

中谷和弘らは、タリンマニュアルの各国での評価はまだ不十分と判断している。

「諸国家としては、サイバー攻撃をめぐる状況がどう推移するか不明確な現状において、「規則○○は慣習国際法になっているが、規則 XX は慣習国際法になっていない」といった何らかの見解を表明することが、将来自国にとって不利な証拠となることを恐れて慎重になっているのかもしれない。」

国連では、サイバーセキュリティに関する政府専門家会合（GGE）が 2004 年以来、 5 会期にわたって検討をしてきたが、サイバー空間に国際法が適用されることについては共通の了解が得られたものの、西側諸国と中国・ロシア等との見解の対立等から、国際法の実体内容の詳細については目立った成果はなかった。

国際法関連：国連

国連、サイバーセキュリティに関する第6会期国連政府専門家会合（the Group of Governmental Experts (GGE) ）

外務省：サイバーセキュリティに関する国連オープン・エンド作業部会（OEWG）

正式名称は国際安全保障の文脈における情報及び電気通信分野での発展に関するオープン・エンド作業部会。2018年12月、第73回国連総会決議（A／RES／73／27）に基づき、国際安全保障の文脈における情報および電気通信分野の発展に関して国連全加盟国参加可能な議論の場として、2019年より国連の下に初めて立ち上がった。同年9月に第1回会合を開催し、全部で3回の本会合を経て本年の国連総会（第75回国連総会）において報告書を提出することとなっている。

※ 報告書

※ 第５会期は報告書を出せずに失敗している

(参考)

サイバー規範に関する国連GGEの失敗

国連GGE2020-21報告書速報を分析する-タリンマニュアルを越えているのか

GGE報告書の主要なポイント（速報版）

1 導入

○本報告書は、過去のGGE報告書に基づき、またその評価と勧告を再度確認する。GGEは、OEWGにおける報告書のコンセンサス採択を歓迎する。

2 既存及び潜在的な脅威

○世界のデジタル化が巨大な機会を提供する一方で、悪意あるサイバー活動を巡る事案が増加。GGEは、多くの国家が軍事目的でICT能力を高めていることを強調。また、国家の悪意あるサイバー活動が他国の安定に影響を与える隠された情報キャンペーンを可能としていることに留意。

3 規範、ルール、責任ある国家の行動原則

○GGEは、新たな規範の追加の可能性を再確認し、適切な場合には、追加的に拘束力のある義務を将来的に検討する可能性に留意した。GGEは、2015年報告書に記載された11の規範について、追加的な理解を発展させた。

ーアトリビューション：被害国と嫌疑のある国は関係当局間で相談することが奨励される。被害国は、事案を評価する際に、堅固な事実に支えられた全ての側面を考慮にいれるべきである。

ー自国領域の使用：この規範は、国家がその領域から国際違法行為が行われていると認識した際に合理的に実施可能で適切な手段を取るであろうという期待を反映している。この規範は、国家がその領域の中で他の国家や非国家主体に国際違法行為を行うためにICTを使うことを許容すべきでないとの理解を伝えている。

ー人権の尊重：オンラインでもオフラインでも、国家はそれぞれの義務に従って、人権や基本的自由を尊重すべき。国家による恣意的な大規模監視はプライバシーをはじめとする人権に特に否定的な影響を与えるかもしれない。

国際法関連：国連

(外務省 2021年 https://www.mofa.go.jp/mofaj/press/release/press24_000114.html)

5月24日から28日まで、サイバーセキュリティに関する第6会期国連政府専門家会合（the Group of Governmental Experts (GGE) ）最終会合が行われ、サイバー空間における責任ある国家の行動に関する報告書が採択(赤堀毅国連・サイバー政策担当大使（総合外交政策局審議官）他がオンラインで出席

本報告書は、サイバー空間における脅威認識、規範、国際法の具体的適用、信頼醸成、能力構築などについて、国連事務総長の委託を受けた25名の政府専門家の共通認識を示すもの

今回の報告書では、国連憲章を含む既存の国際法がサイバー空間に適用されることが再確認され、我が国として重視してきた国際人道法の適用の明記や、国連憲章で認められた国家固有の権利の確認など、国際法のサイバー空間への具体的な適用について議論が進展た。

自国領域の使用、人権の尊重、重要インフラの保護、ICTサプライチェーン等の国家の行動規範についても追加的な理解が深まりました。

今回合意が成立した最終報告書については、本年の国連総会（第76回国連総会）に提出される見通しです。

外務省としても、引き続き、サイバー空間の安全を確保していくため、様々な分野において取組を進めていく考えです。

（参考1）サイバーセキュリティに関する第6会期国連政府専門家会合（GGE）

2018年12月、第73回国連総会決議（A／RES／73／266）に基づき、国際安全保障の文脈におけるサイバー空間での責任ある国家の行動の進展に関して25か国からの専門家（25名）による専門的な議論の場として、国連の下に立ち上がった会合。GGEは過去5会期にわたり実施されている。今会期においては、2019年12月に第1回会合を開催し、全部で4回の本会合を経て本年の国連総会（第76回国連総会）において報告書を提出することとなっている。

国際法関連：国連

外務省：サイバーセキュリティに関する国連オープン・エンド作業部会（2021年－2025年）第1回会合の開催

令和3(2021)年12月20日

12月13日から17日まで、ニューヨーク（国連本部）において、サイバーセキュリティに関する国連オープン・エンド作業部会（the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025（OEWG 2021－2025））第1回会合が開催されました。

　OEWGは、全国連加盟国がサイバー空間における脅威認識、規範、国際法の適用、信頼醸成、能力構築など幅広い議論を行う会合として、2019年に立ち上がり本年3月に報告書を採択しました。更に、昨年提出された国連総会決議に基づき改めて本年から2025年までの期間設置されることが決まったものです。

　12月14日、本件会合の冒頭セッションにおいて、有馬裕サイバー政策担当大使（総合外交政策局審議官）がビデオステートメントを行いました。本ステートメントでは、サイバー空間が経済及び社会的な活動全般において不可欠な公共空間になっており、同空間への攻撃は安全保障上の重大なリスクとなり得る旨の認識を示した上で、同空間に既存の国際法が適用されるとの立場を改めて述べ、従来の国連GGE及びOEWG報告書を含む成果に基づいてOEWG 2021－2025で議論を行っていくべきこと等について強調しました。

ここでいう2019年3月の報告書

https://www.mofa.go.jp/mofaj/press/release/press24_000114.html

https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

国際法関連：国連

マイクロソフト社のコメント「国連がサイバーセキュリティ分野で責任ある国家の行動について合意」
2021年4月22日 | Japan News Center
https://news.microsoft.com/ja-jp/2021/04/22/210422-un-working-group-cybersecurity-report/

- この報告書により、サイバー空間における国際法と、2015 年に自主的な基準として採択されていた責任ある行動規範の権威が高まり支持されるようになること
- この報告書で医療サービスや医療施設などのヘルスケアをサイバー攻撃から守る必要性を説いていること。世界的なパンデミックが続く中、サイバー攻撃によって米国や世界中の病院および医療機関が攻撃されている。
- 情報通信技術 (ICT) のサプライチェーンを保護するよう各国に呼びかけていること。SolarWinds への Nobelium 攻撃は、サプライチェーン攻撃の最新事例で、広範囲に影響が及んだ許されない攻撃でした。Nobelium は、ソフトウェア更新プロセスを破壊し、何千人もの個人や組織を不当な危険にさらしました。このような攻撃により、一般ユーザーは、全ベンダーがデジタルエコシステムのセキュリティを維持するために利用している更新プロセスへの信頼と信用を失う恐れがあります。

「OEWG の報告書は励みになりますが、国連加盟国にはさらなる行動を起こしてもらいたいと思う分野があります。それは人権についてです。この報告書では、残念ながら人権に関する記述は概要のみで、国際人道法については全く触れられていません。この件については、物理的な世界と同様、サイバー空間でも支持されるべきものです。」

国際法関連:国連

2021 年 5 月 28 日

外務省「サイバー行動に適用される国際法に関する日本政府の基本的な立場」

https://www.mofa.go.jp/mofaj/files/100200951.pdf

位置づけと目的

- 2004 年から 2017 年までの間、国連事務総長によって任命された政府専門家からなる「国際安全保障の文脈における情報通信分野の発展に関する政府専門家グループ」（以下 GGE）が国連総会決議に基づき設置された。
- 政府専門家のコンセンサスで作成された 2013 年及び 2015 年の報告書において、特に国連憲章全体を含む、既存の国際法がサイバー行動1にも適用されることが確認
- 2015 年の報告書において、GGE は国際法がサイバー行動にどのように適用されるかにつき、様々な重要な見解を示し、同時に、この議論が継続されるべきである旨を勧告
- 5 回 GGE では 2017 年に報告書を採択できなかった
- 2019 年から、第 6 回 GGE2(「国際安全保障の文脈の中でサイバー空間における国家の責任ある行
- 動を促進することに関する政府専門家グループ)において、国際法がどのように適用されるかに関する議論が活発に行われた。本年 5 月 28 日に第 6 回 GGE の報告書がコンセンサス採択

国際法関連:国連

「サイバー行動に適用される国際法に関する日本政府の基本的な立場」(続)

サイバー行動に適用される国際法

サイバー犯罪に関する条約、CPTPP、日米デジタル貿易協定、日英 EPA 等でルール化を進めている DFFT に関する条約上の規定

- 武力行使の禁止

サイバー行動であっても、一定の場合には、国連憲章第 2 条 4 が禁ずる武力による威嚇又は武力の行使に当たり得る。同条に基づき、すべての国家は、その国際関係において、武力による威嚇又は武力の行使を慎まなければならない。日本政府は、武力による威嚇とは、一般に、現実にはまだ武力を行使しないが、自国の主張、要求を入れなければ武力を行使するとの意思、態度を示すことにより、相手国を威嚇することをいうと考えている。国際関係における武力による威嚇又は武力の行使を慎む義務はサイバー行動に関する重要な義務である。

- 自衛権

サイバー行動が、国際連合憲章 51 条にいう武力攻撃に当たる場合には、国家は、国際連合憲章第 51 条において認められている個別的又は集団的自衛の固有の権利を行使することができると考えられる。

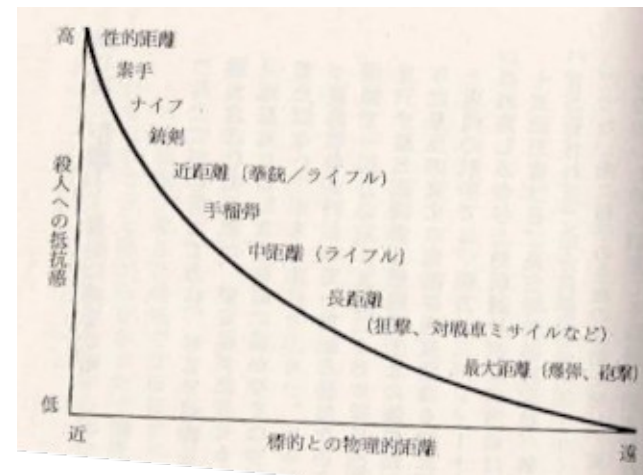
まとめ

- サイバー領域ではNATOとの関係が特に緊密になっている。緊密になりやすい、ともいえる。
- 関連文書や自衛隊、外務省の行動などでは、憲法9条に基く日本の軍事・安全保障における特別な立場を強調することはない。つまり、諸外国の軍隊と同じ立場、条件で行動することを前提とした取り組みになっている。
- サイバー戦争の国際法の枠組はまだ未成熟。国連は、ロシア、中国vs。G7+NATOの対立によって、国際法のグローバル・スタンダードを策定する能力を失なっているようにみえる。
- 他方で、NATOは、国連に先立って、タリン・マニュアルなど独自のルールを先行して策定してグローバル・スタンダードで主導権を握ろうとしているが、結果として、サイバー戦争における「何が違法な戦争なのか」があいまいなまま戦争が継続することになる。
- サイバー分野では、民間企業や政府の非軍事部門、とりわけ情報通信やAIなどの分野が自衛隊やNATOなど海外の軍事組織との連携をかなり深めている。その反面、こうした動きを監視し、牽制する平和運動の力が世界的にみても極めて弱い。

まとめ

なぜサイバー領域での「戦争放棄」が不十分なのか

- 軍事と非軍事の境界があいまい。従来の軍事産業や武器の概念にとらわれるとサイバー領域での戦争体制に対抗できない。
- 標的との物理的距離が遠いほど殺人への抵抗感が薄くなることが知られている。(デーブ・グロスマン『戦争における「人殺し」の心理学』(ちくま学芸文庫)

サイバー領域は最も「距離」が遠いために、戦争=殺人への倫理的な判断が最も鈍くなる。このことが、反戦・平和運動においても課題として「二の次」とみなされやすい。この課題を解決する必要がある。

まとめ

サイバー戦争は私たちのコミュニケーション手段と、これを支えるインフラをまるごと戦争体制に組み込むことになる。まず、危機感をもつことが大切だと思います。そこから、何をすべきか、何ができるか、という問いへの答え捜しも始められるのではないかと思います。